PM 2006 RI (Dnr 034-4526/2005)

Tillämpningsanvisningar och instruktioner för informationssäkerhet i Stockholms stad

Borgarrådsberedningen föreslår kommunstyrelsen besluta följande

Tillämpningsanvisningar och instruktioner för informationssäkerhet i Stockholms stad godkänns.

Föredragande borgarrådet Annika Billström anför följande.

Ärendet

I detta ärende anmäls den första versionen av Anvisningar och Instruktioner för informationssäkerhet i Stockholms stad - *bilaga*. Till grund för anvisningarna ligger kommunfullmäktiges beslut tidigare i år om Policy och Riktlinjer för informationssäkerhet i Stockholms stad.

Ärendets beredning

Ärendet har beretts av stadsledningskontoret.

Mina synpunkter

Som tidigare konstaterades i samband med beslutet i kommunfullmäktige om policy och riktlinjer för stadens informationssäkerhet är en väl fungerande informationshantering en väsentlig förutsättning för Stockholms stads verksamhet. Den reviderade policyn med därtill hörande tillämpningsanvisningar och instruktioner för ökad IT-säkerhet är en viktig förutsättning för att uppnå en tillräckligt hög grad av säkerhet i stadens IT-baserade system.

Jag föreslår kommunstyrelsen besluta följande

Tillämpningsanvisningar och instruktioner för informationssäkerhet i Stockholms stad godkänns.

Stockholm den 9 januari 2006

ANNIKA BILLSTRÖM

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

ÄRENDET

I detta ärende anmäls den första versionen av Anvisningar och Instruktioner för informationssäkerhet i Stockholms stad - *bilaga*. Anvisningarna är ett levande dokument och förvaltningen skall ske genom stadens Informationssäkerhetschef. Till grund för anvisningarna ligger kommunfullmäktiges beslut tidigare i år om Policy och Riktlinjer för informationssäkerhet i Stockholms stad.

Bakgrund

Mot bakgrund av en ökad och i viss mån förändrad hotbild, den tekniska utvecklingen och inte minst stadens ambition att vara en s.k. 24-timmarskommun har ett nytt förslag till policy och riktlinjer för informationssäkerhet för Stockholms stad utarbetats.

Kommunfullmäktige fattade den 13 juni 2005 beslut att godkänna förslag till policy och riktlinjer för informationssäkerhet i Stockholms stad. Därutöver uppmanades Stockholms Stadshus AB att anta policy och riktlinjer för informationssäkerhet inom koncernen. Kommunstyrelsen fick i uppdrag att utfärda tillämpningsanvisningar och instruktioner för informationssäkerhet i Stockholms stad, vilka i detta ärende anmäls.

Motivet för och avsikten med denna typ av dokument är att kommunkoncernen skall hantera säkerhetsfrågor kring informationshantering på ett enhetligt sätt och att staden skall verka för en homogen och trygg hantering av såväl integritetskänslig information som annan ur verksamhetssynpunkt väsentlig information.

I enlighet med målet för stadens e-strategi produceras idag nya elektroniska tjänster till medborgare, nya funktioner för samarbetspartners och kunder till staden samt för stadens anställda. I takt med den tekniska utvecklingen, exempelvis mobilitet och trådlös kommunikation uppstår också krav på nya säkerhetslösningar. Ett regelverk för säkerhet måste därför idag omprövas oftare än tidigare.

Ärendets beredning

Ärendet har beretts av stadsledningskontoret då kommunstyrelsen gav stadsdirektören i uppdrag att utfärda tillämpningsanvisningar och instruktioner för informationssäkerhet för Stockholms stad.

Stadsledningskontorets tjänsteutlåtande daterat den 28 november 2005 har i huvudsak följande lydelse.

En väl fungerande informationshantering är en väsentlig förutsättning för Stockholms stads effektivitet. Informationssäkerhetsarbetet bidrar till en tryggad informationshantering. Det måste ske förebyggande, på lång sikt och för att vara effektivt och heltäckande, genomföras väl strukturerat och med tydligt stöd från verksamhetsledningen.

För att uppnå en trygg och effektiv informationshantering vid Stockholms stad krävs en enhetlig syn på säkerhetsbedömningar och åtgärder. Gemensamma styrande dokument är ett medel för att uppnå en homogen, grundläggande utgångspunkt och ge likvärdiga förutsättningar för säkerhetsarbetet.

Kommunfullmäktige beslutade den 13 juni 2005 att godkänna Policy och Riktlinjer för informationssäkerhet i Stockholms stad. Detta dokument anger en viljeinriktning och beskriver vilka frågor som är av överordnad betydelse. Beslutet omfattade också ansvaret att fastställa tillämpningsanvisningar och instruktioner vilket skulle tilldelas kommunstyrelsen och verkställas genom stadsdirektören.

Bilagda dokument är den första versionen av Anvisningar och Instruktioner för området. Anvisningarna skall vara ett levande dokument och förvaltningen skall ske genom stadens Informationssäkerhetschef.

Bilaga

Appendix A - Anvisningar och instruktioner för informationssäkerhet i Stockholms stad.

Bilaga

Appendix A

Anvisningar och instruktioner för Informationssäkerhet Stockholms stad

Utfärdat av Stadsdirektören **2005-11-30**

INNEHÅLLSFÖRTECKNING

1 Inledning och omfattning

1.1 Inledning

En väl fungerande informationshantering är en väsentlig förutsättning för Stockholms stads effektivitet.

Informationssäkerhetsarbetet bidrar till en tryggad informationshantering. Det måste ske förebyggande, på lång sikt och för att vara effektivt och heltäckande, genomföras väl strukturerat och med tydligt stöd från verksamhetsledningen.

Förankringen och medvetandet hos medarbetarna utgör själva grunden för informationssäkerhetsarbetet.

Informationssäkerhet handlar om

- **sekretess**, skydd mot obehörig åtkomst av information
- **riktighet**, åtgärder för att åstadkomma rätt kvalitet på information
- **tillgänglighet**, åtgärder för att säkra drift och funktionalitet
- **spårbarhet**, möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse

Säkerhet åstadkoms genom många samverkande faktorer, inte en avancerad teknikkomponent eller en enstaka säkerhetsåtgärd.

Rätt säkerhetsnivå uppnås när:

- system/information har klassificerats och aktuella krav är uppfyllda
- riskanalyser och säkerhetsuppföljningar har genomförts och identifierade brister åtgärdats.

Detta innebär även att Revisionskontorets krav på säkerheten i stadens IT-system, ur internkontrollsynpunkt, är uppfyllda.

Informationssäkerhetsinsatser skall bidra till att **rätt person**
har tillgång till **rätt information**
i **rätt tid.**

1.2 Omfattning

Säkerhetsarbetet omfattar alla åtgärder vars samlade effekt är att förebygga och begränsa konsekvenserna av störningar för informationshantering inom verksamheter i koncernen Stockholms stad.

Personer som omfattas är förtroendevalda, anställda och i viss omfattning skolelever samt konsulter/entreprenörer om uppdragens karaktär är relevanta för informationssäkerheten.

1.2.1 Processinriktning

PDCA (PlanDoCheckAct)är en modell (hämtad från standarden Ledningssystem för InformationsSäkerhet [LIS], SS-ISO/IEC 17799) som utgör grunden för informationssäkerhetsarbetet i Stockholms stad.

Standarden förordar tillämpning av processinriktning för att etablera, införa, driva, följa upp, granska, upprätthålla och förbättra effektiviteten i detta informationssäkerhetsarbete.

Målet är att uppnå ständiga förbättringar.

1.3 Dokumentstruktur och roller

Dokumentet bygger på en hierarki utgående från begreppen **Policy, Riktlinjer, Anvisningar** och **Instruktioner** och med en kapitelindelning som följer SS-ISO/IEC 17799.

- Policyn formuleras på en övergripande nivå och uttrycker ledningens viljeinriktning

- Riktlinjer anger VAD som skall göras och pekar ut ansvar, säkerhetsprocesser och mål

- Anvisningar anger HUR skydd skall införas och vilka säkerhetsåtgärder som skall vidtas
- Instruktioner är detaljerad information till Anvisningarna.
Policy och Riktlinjer (rubriknivå X.X.X) återfinns i huvuddokumentet (Policy och Riktlinjer för Informationsssäkerhet) medan Anvisningar (rubriknivå X.X.X.X) och Instruktioner är samlade i detta Appendix A. Vid behov kan lokal anpassning av Appendix A göras och detta beslutas av respektive nämnd eller styrelse.
Dokumentet utgör en samlad bild av informationssäkerheten inom staden.
Den roll man representerar avgör vilka delar av dokumentet som är tillämpliga.
I nedanstående tabell visar **+** markeringar vilka kapitel som är de mest väsentliga för respektive roll. Rollerna beskrivs i kapitel 4.

Roll **Kapitel**	**System-ägare**	**Förv.-Bolags-V-ansv chef**	**System-ägar-repre-sentant**	**An-vänd-are**	**IT-chef**	**Tek-nisktsys-tem-ansvarig**	**Extern tjänste-leve-ran-tör**	**Info.säker-hetschef/-samordn.**
1 Inledning/ Omfattning	+	+	+	+	+	+	+	+
2 Termer/ Definitioner	+	+	+	+	+	+	+	+
3 Policy	+	+	+	+	+	+	+	+
4 Organisatorisk säkerhet	+	+	+	+	+	+	+	+
5 Klassificering och styrning av tillgångar								
Riktlinjer	+	+	+	+	+	+	+	+
Anvisningar	-	-	+	-	+	-	-	+
6 Personal och säkerhet								
Riktlinjer	+	+	+	+	+	-	+	+
Anvisningar	-	+	+	-	+	-	-	+
7 Fysisk och miljörelaterad säkerhet								
Riktlinjer	-	+	+	-	+	+	+	+
Anvisningar	-	-	+	+	+	+	+	+
8 Styrning av kommunikation och drift								
Riktlinjer	-	-	+	-	+	+	+	+
Anvisningar	-	-	-	+[1]	+	+	+	+
9 Styrning av åtkomst								
Riktlinjer	-	+	+	-	+	+	+	+
Anvisningar	-	-	-	+	+	+	+[1]	+
10 Systemutveckling /-anskaffning och /-underhåll								
Riktlinjer	-	-	+	-	+	+	+	+
Anvisningar	-	-	-	-	+	+	+	+
11 Kontinuitets- och avbrottsplanering								
Riktlinjer	+	+	+	-	+	+	+	+
Anvisningar	-	+	+	-	+	+	+	+
12 Efterlevnad Riktlinjer	+	+	+	+	+	+	+	+
Anvisningar	+	+	+	+	+	+	-	+

[1] Valda delar av innehållet

1.4 Avgränsningar

Inga avgränsningar finns utan dokumentet är tillämpligt för all informationshantering, oberoende av media.

1.5 Styrande dokument

Säkerhetspolicyför Stockholms stad, Brandförsvaret	KF 1993-09-06
e-strategi	KF 2001-02-19
Informationsteknisk plattform (ITP)	KF 2005-02-21

2 Termer och definitioner

2.1 Termer

Beskrivning av termer som påverkat utformningen av och innehållet i detta dokument.

SS-ISO/IEC 17799	**L**edningssystem för **I**nformations**S**äkerhet **(LIS)** är en internationell standard som omfattar riktlinjer eller ”code of practice” för ledning av informationssäkerhet. Standarden ger råd om hur man på ett strukturerat och systematiskt sätt styr informationssäkerhetsarbetet i en verksamhet.
PDCA	PlanDoCheckAct (PDCA) är en modell som bygger på ett ramverk av riktlinjer för hur ett **LIS** fungerar.
OffLIS	Vägledning och mallregelverk för **LIS** för 24-timmarsmyndigheter.

2.2 Definitioner

Begrepp	Beskrivning
Policy	Anger ledningens viljeinriktning och stöd för informationssäkerhet. Policyn beskriver ”att något ska finnas”.
Riktlinjer	Anger VAD som skall göras för att uppfylla de övergripande målen i policyn.
Anvisningar	Anger på en funktionell nivå HUR (på vilket sätt) skyddsåtgärder och administrativa processer skall utformas.
Instruktioner	Ges för specifika system och/eller anvisningar. Instruktioner beskriver "hur och av vem" anvisningarna ska införas/följas.
Användare	Individ som utnyttjar informationstillgångar.
Autenticering	Verifiering av uppgiven identitet.
Avbrottsplan [IT]	Plan för att kunna återuppta driften efter driftstörning eller då IT-system inte fungerar som avsett. Avbrottsplanen baseras på vad som beskrivs i kontinuitetsplanen.
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.
Identitet	Unik beteckning för en viss individ.
Incident	Säkerhetshändelse som kan/kunnat få/har fått allvarliga konsekvenser för verksamheten.
Informations-klassificering	Ett formellt sätt att fastställa rätt skyddsnivå för ett IT-system. Uttrycks i en s.k. säkerhetsprofil**.**
Informations-säkerhet	Säkerhet beträffande informationstillgångar avseende förmågan att upprätt-hålla önskad åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet.
Informations-tillgångar	En organisations informationsrelaterade tillgångar, vilka har ett värde för organisationen och därmed är skyddsvärda. *Exempel på informationstillgångar är:* *Information (databaser, filer, metodik, dokument, etc.)* *Program (tillämpningar, operativsystem, etc.)*

	Tjänster (nätförbindelser, abonnemang, etc.) *Fysiska tillgångar (datorer, datamedia, lokala nätverk, etc.)*
IT-system	Är en konstellation av datorer, in- och utmatningsutrustning, minnesenheter, program, kommunikationsutrustningar, metoder och procedurer organiserade med uppgift att genomföra elektronisk behandling av information i syfte att tillgodose ett uttalat behov.
Kontinuitets-plan [för verksamheten]	Dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.
Logg	Insamlad information om de operationer som utförs i ett IT-system. Tre typer av loggar är aktuella: Säkerhetslogg, driftlogg och transaktionslogg.
Riktighet	Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats.
Risk	Produkten av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad.
Riskanalys	Process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder.
Sekretess	Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga. Begreppet ersätts med **Åtkomstbegränsning** i detta dokument.
SLA [Service Level Agreement]	Dokument som reglerar vad som överenskommits mellan systemägar-representant och IT-chef gällande drift och förvaltning av visst IT-system.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i IT-systemet till en identifierad användare. För att åstadkomma spårbarhet krävs åtminstone identifiering och autenti-cering av användare samt loggning av relevanta händelser i IT-systemet.
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot.
Säkerhet	Egenskap eller tillstånd som innebär skydd mot risk i samband med insyn, förlust eller påverkan; oftast i samband med medvetna försök att utnyttja eventuella svagheter.
Säkerhetsprofil	Alla IT-system har ett skyddsbehov. Skyddsbehovet varierar beroende på typ av informationstillgång. Genom att klassificera informationen med avseende på åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet erhålls en säkerhetsprofil. Denna avgör vilka säkerhetskrav som ställs på informationstillgången.
Tillgänglighet	Möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad tid.
Åtkomst-/behörighets-kontroll	Syftar till att reglera och kontrollera en användares åtkomst till olika informationstillgångar samt att skydda information och program, så att de endast är tillgängliga utifrån tilldelad (roll-)behörighet.

3 Informationssäkerhetspolicy

För att uppnå en trygg och effektiv informationshantering vid Stockholms stad krävs en enhetlig syn på säkerhetsbedömningar och åtgärder.

Gemensamma styrande dokument är ett medel för att uppnå en homogen, grundläggande utgångspunkt och ge likvärdiga förutsättningar för säkerhetsarbetet.

Avsikten med denna policy är att skydda stadens informationstillgångar mot alla hot – interna eller externa, avsiktliga eller oavsiktliga.

Via riskanalyser fastställs rätt avvägd riskkostnad, dvs säkerhetsåtgärderna skall vara ekonomiskt försvarbara.

Följande inriktning gäller:

- Stadens styrande dokument skall vara kända
- Stadens säkerhetsorganisation skall vara känd
- Grundnivån för säkerheten skall fastställas genom informationsklassificering
- Berörd personal skall ha nödvändiga kunskaper om aktuella IT-system och gällande säkerhetsregler
- Fysiskt skalskydd skall anpassas efter genomförd riskanalys
- Skriftligt godkänt SLA/motsvarande skall finnas före driftsättning
- Åtkomst/behörighet skall tilldelas formellt och endast efter behov samt följas upp regelbundet
- Säkerhetsaspekter skall beaktas vid utveckling och anskaffning av IT-system
- Uppfyllnad av rättsliga krav skall tillgodoses i alla IT-system
- Kontinuitetsplan skall finnas för verksamheter med starkt beroende av IT-system
- Alla incidenter skall rapporteras och kontinuerlig uppföljning skall ske mot fastställda regler

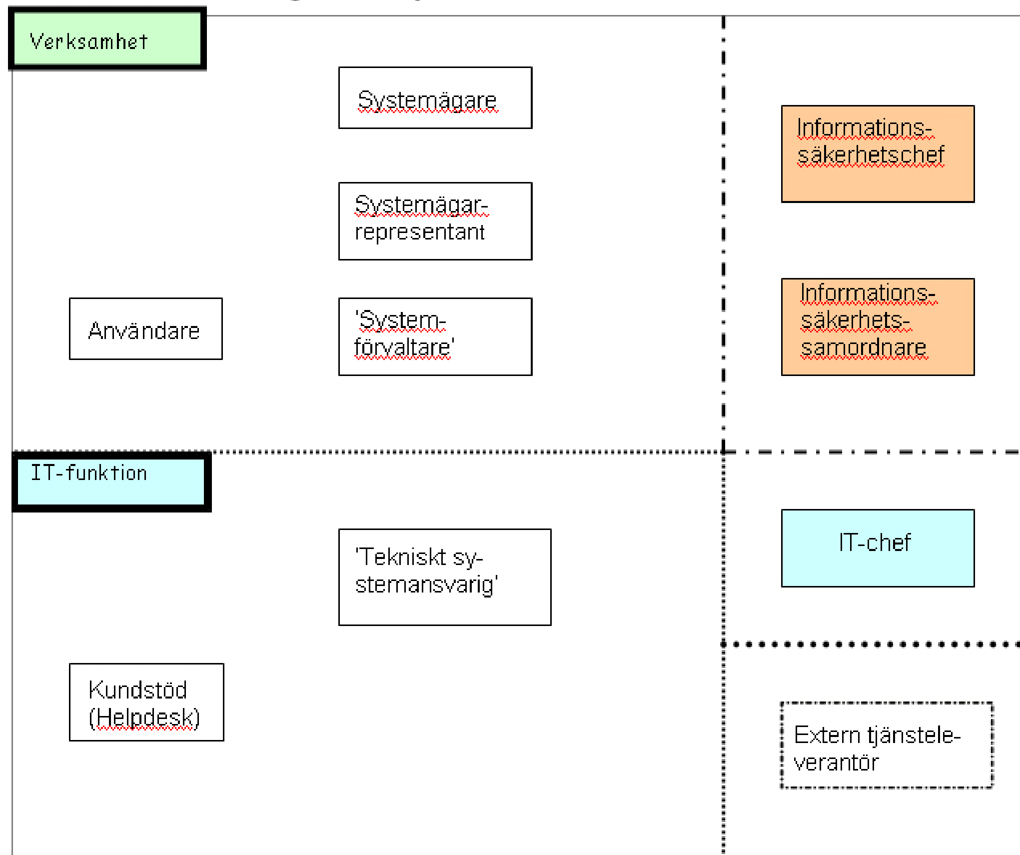
4 Organisatorisk säkerhet

4.1 Infrastruktur för informationssäkerhet

Nedan beskrivs schematiskt de viktigaste rollerna vid drift och förvaltning av IT-system.

I nedanstående figur skall informationssäkerhetschef och informationssäkerhetssamordnare enbart ses som oberoende intressenter.

Roll- och ansvarsfördelning mellan central och lokal instans framgår inte.



4.2 Roller

Aktuella roller finns beskrivna i huvuddokumentet Policy och Riktlinjer undantagandes rollen Kundstöd.

5 Klassificering och styrning av tillgångar

Ansvarig för information eller informationstillgångar skall också ansvara för att klassificering görs och att konstaterade säkerhetskrav tillgodoses.

5.1 Ansvar för tillgångar

5.1.1 Förteckning över tillgångar

Informationstillgångar skall vara förtecknade och i vissa fall även vara märkta.

5.1.1.1 *Anvisningar för förteckning och märkning av tillgångar*

Pos	Text	Koppling till Instruktioner
Allmänt	Informationstillgångar representerar stora värden och måste hållas noggrant uppdaterade.	
5.1.1.1-1	Informationstillgångar skall vara dokumenterade och ansvariga utsedda.	5.1.1.1-1. I1 5.1.1.1-1. I2
5.1.1.1-2	Utrustning, i synnerhet stöldbegärlig, skall vara märkt.	5.1.1.1-2. I1

Instruktioner för förteckning och märkning av tillgångar

5.1.1.1-1.I1

Förteckning av programvara – exempel på mall i excel-format återfinns under [http://info.slkit.stockholm.se/templates/page.asp?id=888].

5.1.1.1-1.I2

Förteckning av datorutrustning – exempel på mall i excel-format återfinns under [http://info.slkit.stockholm.se/templates/page.asp?id=888].

5.1.1.1-2.I1

Stöldskyddsmärkning skall ske på sådant sätt att märkning inte går att avlägsna. Rekommenderade metoder är gravyr och etsning.

5.2 Klassificering av information

5.2.1 Riktlinjer för informationsklassificering

Informationstillgångar skall klassificeras (värderas) så att rätt skyddsnivå kan fastställas.

Klassificering skall ske tidigt i samband med systemutveckling/-anskaffning och återkommer i förvaltningsskedet.

Klassificeringen utgår från faktorerna Åtkomstbegränsning, Riktighet, Tillgänglighet och Spårbarhet.

Av staden fastställd metod för informationsklassificering skall användas.

5.2.1.1 *Anvisningar för informationsklassificering*

Pos	Text	Koppling till Instruktioner
Allmänt	Syftet med att klassificera informationstillgångar är att säkerställa att de ges ett tillräckligt skydd. Att klassificera information är en grundläggande aktivitet för att särskilja den information som ställer högre krav på säkerhet. Förutom legala krav på skydd skall verksamhetens bedömning av informationens värde avseende åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet avgöra omfattningen av det skydd som skall uppnås.	
5.2.1.1-1	Informationsklassificering skall ske enligt gällande Handbok för Informationsklassificering.	5.2.1.1-1.I1

Instruktioner för informationsklassificering

5.2.1.1-1.I1

Handbok för informationsKLassificering (HKL) ger en detaljerad beskrivning av hur en informationsklassificering genomförs.

5.2.2 Märkning och hantering av information

Information som är belagd med sekretess skall märkas så att detta framgår.

Det skall även framgå om informationen utgör original eller kopia.

Sekretessprövning skall föregå beslut om utlämnande av information som kan bli föremål för sekretessmärkning.

Hemlig information enligt sekretesslagen 2 kap 2§ hanteras ej i detta dokument.

5.2.2.1 *Anvisningar för märkning och hantering av information vid sekretess*

Pos	Text	Koppling till

		Instruktioner
Allmänt	Stadens informationshantering styrs främst av bestämmelser i tryckfrihetsförordningen och sekretesslagen. Huvudregeln i denna lagstiftning är att informationen skall vara tillgänglig för allmänheten, den s k offentlighetsprincipen. Undantag från huvudregeln utgör information som med stöd av reglerna i sekretesslagen kan omfattas av sekretesskydd. Det är väsentligt att varje anställd har kännedom om vilken information inom i första sitt eget ansvarsområde som är sekretessbelagd och hur den skall hanteras. Prövning av sekretess föreligger för viss information varje gång begäran om utlämning av handling görs. Detta oavsett om handlingen är sekretessbelagd eller ej. Nedanstående anvisningar omfattar ej sekretess gällande rikets säkerhet enligt Sekretesslagen 2 kap. För sådana situationer hänvisas till stadens säkerhetsskyddschef.	
5.2.2.1-1	Sekretessbelagda handlingar kan märkas med särskild stämpling/påteckning.	5.2.2.1-1.I1
5.2.2.1-2	Sekretessbelagda handlingar skall förvaras i säkerhetsskåp.	5.2.2.1-2.I1
5.2.2.1-3	Sekretessbelagda handlingar skall vid gallring förstöras i dokumentförstörare.	---

5.2.2.1-4	Sekretessbelagda handlingar skall distribueras med bud eller rekommenderat brev med mottagningsbevis.	---
5.2.2.1-5	Sekretessbelagda handlingar i elektronisk form skall distribueras krypterade om teknisk plattform medger detta.	5.2.2.1-5.I1
5.2.2.1-6	Sekretessbelagda handlingar i elektronisk form skall, om särskilda verksamhetskrav ställs, lagras krypterade om teknisk plattform medger detta.	5.2.2.1-6.I1
5.2.2.1-7	Respektive chef skall säkerställa korrekt hantering av sekretessbelagda handlingar.	---

Instruktioner för märkning och hantering av information vid sekretess

5.2.2.1-1.I1

Hur märkning skall ske framgår av Sekretesslagen 15 kap 3§.

5.2.2.1-2.I1

Säkerhetsskåp skall uppfylla Stöldskyddsföreningens norm SS 3492.

5.2.2.1-5.I1

Det framgår i ITP (4.5.2) hur detta sker.

5.2.2.1-6.I1

Av staden rekommenderad lösning (via tredje part) skall användas.

5.2.2.2 *Anvisningar för hantering av arbetsmaterial*

Pos	Text	Koppling till Instruktioner
Allmänt	Arbetsmaterial kan vara av olika slag. Ofta ingår arbetsmaterial i ett pågående ärende tillsammans med Allmänna handlingar. Det skall beaktas att det arbetsmaterial som dagligen hanteras kan resultera i en Allmän handling som kan efterfrågas för utlämnande.	
5.2.2.2-1	Arbetsmaterial skall förvaras och distribueras på ett sådant sätt att full kontroll kan upprätthållas och informationen i arbetsskedet inte kan komma obehörig till hands.	---
5.2.2.2-2	I samband med resor, konferenser och motsvarande skall arbets-material hanteras på sådant sätt att exponering för obehöriga undviks.	---

6 Personal och säkerhet

Genom säkerhetsinsatser skall riskerna minskas för mänskliga misstag, stöld, bedrägeri och missbruk av informationstillgångar.

Målgruppen i kapitlet är förutom anställda i vissa fall även förtroendevalda och konsulter/entreprenörer.

6.1 Säkerhet vid rekrytering och för anställd personal

6.1.1 Krav på anställda gällande informationssäkerhet

Förhållanden och villkor för anställning skall klart uttala den anställdes ansvar för informationssäkerhet.

6.1.1.1 *Anvisningar gällande personal och säkerhet*

Pos	Text	Koppling till Instruktioner
Allmänt	Alla anställda skall vara medvetna om sitt ansvar vad gäller informationssäkerhet.	
6.1.1.1-1	Uppgifter som lämnas i platsansökningar skall alltid kunna verifieras.	---
6.1.1.1-2	Vid anställning skall kort information ges om den anställdes informationssäkerhetsansvar.	6.1.1.1-2.I1
6.1.1.1-3	Personal i viss verksamhet skall registerkontrolleras enligt gällande lagstiftning.	6.1.1.1-3.I1
6.1.1.1-4	Personal som kan komma i kontakt med sekretessbelagda handlingar skall informeras om Offentlighetsprincipen och Sekretesslagen.	---
6.1.1.1-5	Om person slutar sin anställning eller övergår till annan befattning inom staden skall lokala instruktioner finnas som styr avveckling/förändring av åtkomst till såväl lokaler som IT-system.	---
6.1.1.1-6	För personal med högre behörigheter till lokaler och IT-system och där uppsägning/övertalighet är aktuell rekommenderas att dessa behörigheter omedelbart inaktiveras.	---
6.1.1.1-7	Tystnadsförbindelse skall upprättas för konsulter/entreprenörer med uppdrag inom staden.	6.1.1.1-7.I1
6.1.1.1-8	Vid övertalighet, tjänstledighet > 6 månader och långtidssjukskrivning skall, om inte annat överenskommits, åtkomsträttigheter till system omgående revideras.	---

Instruktioner gällande personal och säkerhet

6.1.1.1-2.I1

Vid nyanställning skall den anställde förbinda sig att ta del av och acceptera gällande regelverk för informationssäkerhet.

6.1.1.1-3.I1

PPA cirkulär 24 beskriver vad som gäller för Registerkontroll.
För registerkontroll enligt Säkerhetsskyddslagen SFS 1996:627 hänvisas till stadens säkerhetsskyddschef vid Brandförsvaret.

6.1.1.1-7.I1

Det åligger beställare/uppdragsgivare att innan uppdragets påbörjan upprätta tystnadsförbindelse.
Tystnadsförbindelse beskrivs på stadens intranät under 'IT i staden/Informationssäkerhet/Policy och regelverk/Tystnadsförbindelse'.

6.1.1.2 *Anvisningar för hantering av e-post*

Pos	Text	Koppling till Instruktioner
Allmänt	Ordningsregler för elektronisk post har fastställts av kommunfullmäktige. (KS utl. 1998:106). Nya regler är under utarbetande. Offentlighetsprincipen, med avseende på diarieföring, och säkerheten i stadens nätverk ställer krav på en korrekt hantering av e-post.	
6.1.1.2-1	E-post skall hanteras enligt de regler som sätts upp av lagar och förordningar (offentlighet och sekretess).	6.1.1.2-1.I1
6.1.1.2-2	E-post skall diarieföras i enlighet med vad som gäller för diarieföring av andra allmänna handlingar.	6.1.1.2-2.I1
6.1.1.2-3	E-post skall omfattas av samma regler och etiska normer som traditionell post.	---
6.1.1.2-4	Automatisk vidarebefordran till publika brevlådor /externa adresser, exempelvis Hotmail, är inte tillåtet.	---
6.1.1.2-5	Automatisk vidarebefordran av e-post till annan brevlåda får endast ske om krav på diarieföring kan tillgodoses.	---
6.1.1.2-6	Anställda inom staden får skicka sekretessbelagda eller integritetskänsliga uppgifter med e-post om säkerhetslösning för detta ändamål stöds av teknisk plattform.	6.1.1.2-6.I1
6.1.1.2-7	Utskick av e-post i massupplaga får endast ske om det är av tjänsten påkallat.	---
6.1.1.2-8	Bifogade filer/bilagor från okänd avsändare skall hanteras med sunt förnuft för att undvika störning/skada (virusrisk) i IT-miljön.	---
6.1.1.2-9	Användning av e-post med stadens e-postadress skall vara relaterat till arbetsuppgifterna.	---

Instruktioner för hantering av e-post

6.1.1.2-1.I1

E-posten skall regelbundet kontrolleras.
E-post av ringa betydelse skall gallras (raderas) snarast möjligt.

6.1.1.2-2.I1

Hänvisning till gällande 'Regler för e-post inom Stockholms stad'.

6.1.1.2-6.I1

Säkerhetslösning skall innefatta kryptering. Detta beskrivs i ITP.

6.1.1.3 *Anvisningar för åtkomst till och användning av Internet*

Pos	Text	Koppling till Instruk-tioner
Allmänt	Internet skall användas som ett hjälpmedel för att lösa arbetsuppgifterna. Betrakta Internet som en av många informationskällor för informationsinhämtning. Använd inte Internet för privat bruk utöver vad som kan jämställas med telefoni- eller litteraturnytt-jande. Nedladdning av filer såsom bild och ljud kräver mycket server-utrymme och bandbredd och är därmed mycket kostnadskrävande för staden.	
6.1.1.3-1	Internet får endast användas inom de regler som sätts upp av lagar och förordningar, exempelvis Upphovsrättslagen och PUL.	---
6.1.1.3-2	Vid användning av Internet skall samma etiska normer gälla som för annan informationshämt-ning/-spridning.	---
6.1.1.3-3	Material som är sekretessbelagt får inte publiceras på Internet.	---
6.1.1.3-4	Det ska alltid finnas en namngiven person – "en ansvarig utgivare" - med övergripande ansvar för att en webbsidas innehåll följer stadens informations-policy och riktlinjer för webbpublicering.	---
6.1.1.3-5	Nedladdning/lagring av bild- och ljudfiler för privat bruk är inte tillåtet.	---
6.1.1.3-6	Kontroll av enskilda personers surfning, e-post och lagrade filer skall ske då misstanke om brott eller missbruk föreligger.	---
6.1.1.3-7	Kontroll av respektive förvaltnings eller bolags surfning skall ske genom stickprov eller på annat vis.	6.1.1.3-7.I1
6.1.1.3-8	Om anställd vid staden deltar i diskussionsgrupper på Internet eller lämnar bidrag till nyhetsgrupper måste vederbörande kunna skilja på stadens officiel-la ståndpunkt respektive sina personliga åsikter.	---

Instruktioner för åtkomst till och användning av Internet

6.1.1.3-7.I1
Respekt för den personliga integriteten skall iakttas. Dock skall stickprovskontroller och analyser av filtyper och kommunikationsflöden genomföras med oregelbundna intervall. Om resultat av kontroll ger upphov till misstankar om oegentligheter skall respektive användare kontaktas för att ges tillfälle till förklaring. Om arbetsledningen konstaterar oegentligheter styrs användandet av eventuella sanktioner av straffrättslig och arbetsrättslig lagstiftning och praxis.

6.2 Användarutbildning

6.2.1 Utbildning i informationssäkerhet

Verksamhetsansvarig chef skall tillse att berörd personal ges möjlighet att genomgå utbildning i informationssäkerhet.

6.2.1.1 *Anvisningar för användarutbildning*

Pos	Text	Koppling till Instruktioner
Allmänt	Utbildning ingår i en kontinuerlig process för att skapa medvetande om informationssäkerhet och gällande säkerhetskrav.	
6.2.1.1-1	Systemägarrepresentanten skall definiera vilka krav som ställs på systemets användare.	---
6.2.1.1-2	Alla användare, liksom även konsulter samt övriga tredjeparts-användare, skall få en anpassad utbildning i informationssäkerhet.	---
6.2.1.1-3	Användardokumentation skall finnas tillgänglig för alla användare.	---

6.3 Säkerhetsincidenter och funktionsfel

6.3.1 Rapportering

Incidenter och säkerhetsmässiga svagheter skall snarast möjligt rapporteras för att initiera nödvändiga åtgärder för att minimera skada, åtgärda brister och utreda eventuell brottslighet.

6.3.1.1 *Anvisningar för incidenthantering*

Pos	Text	Koppling till Instruktioner
Allmänt	Rapportering av incidenter är av stor vikt när man vill skaffa sig en helhetsbild av vad som skall prioriteras ifråga om säkerhetsåtgärder. En väl fungerande incidentrapportering möjliggör att hotbildens relevans kan säkerställas och att på så vis satsningar görs på de viktigaste områdena. Exempel på incidenter som skall rapporteras är virusangrepp, intrång/intrångsförsök och manipulation/radering av information.	
6.3.1.1-1	Alla användare skall rapportera incidenter till informationssäkerhets-samordnaren vilken i sin tur rapporterar vidare till stadens informationssäkerhetschef.	6.3.1.1-1.I1

Instruktioner för incidenthantering

6.3.1.1-1.I1

Stadens standardiserade verktyg för rapportering av incidenter bör användas. Respektive förvaltning/bolag avgör hur den praktiska hanteringen av aktuellt verktyg skall ske.

7 Fysisk och miljörelaterad säkerhet

Säkerhetspolicy för Stockholms stad, (1993-09-06), som Brandförsvaret har förvaltningsansvar för, reglerar övergripande den fysiska säkerheten vid Stockholms stads bolag/förvaltningar. Denna går att läsa på www.brand.stockholm.se, Säkerhet och beredskap/Användbara dokument.

7.1 Säkrade utrymmen

7.1.1 Skalskydd och tillträde

För verksamheten kritiska eller viktiga informationstillgångar skall inrymmas i säkrade utrymmen inom ett avgränsat skalskydd med lämpliga spärrar och tillträdeskontroller.

Nivån på skalskyddet fastställs med hjälp av riskanalys.

Installationer av tillträdesskydd, inbrottslarm och brandlarm skall grundas på auktoriserad organisations normer om sådana finns.

Tillträdeskontroll skall tillämpas för att säkerställa att endast behörig personal får tillträde till säkrade utrymmen.

7.1.1.1 *Anvisningar för skalskydd och tillträde*

Pos	Text	Koppling till Instruktioner
Allmänt	För att upprätthålla en störningsfri drift är det viktigt att begränsa tillträdet till driftmiljön.	
7.1.1.1-1	Branschnormer avseende brand- och stöldskydd skall följas.	7.1.1.1-1.I1
7.1.1.1-2	Servrar och kommunikationsutrustning skall placeras i därför avsedda utrymmen.	7.1.1.1-2.I1
7.1.1.1-3	Godkända lås- och larmsystem, anpassade till aktuell driftmiljö, skall finnas.	7.1.1.1-3.I1
7.1.1.1-4	I sammanhang där känslig/sekretessbelagd information hanteras skall passerkontrollsystem finnas.	---
7.1.1.1-5	Nycklar och passerkort skall förvaras i säkerhetsskåp.	7.1.1.1-5.I1
7.1.1.1-6	Vid hantering av nycklar skall nyckelschema användas.	7.1.1.1-6.I1
7.1.1.1-7	Extern och egen personal, som inte har behörighet, skall vara åtföljda vid tillträde till server- och kommunikationsutrymmen.	---
7.1.1.1-8	Vid externt besök i server- och kommunikationsutrymmen skall loggbok föras.	7.1.1.1-8.I1
7.1.1.1-9	I publika miljöer där datorer tillhandahålls skall inre och yttre skalskydd beaktas.	7.1.1.1-9.I1

Instruktioner för skalskydd och tillträde

7.1.1.1-1.I1

De normer som i första hand är aktuella heter EN 1047 (EU norm för brandklassning) där brandklass P = för pappersdokument och brandklass DIS = för olika typer av datamedia. samt SSF 200:3 (Regler för mekaniskt inbrottsskydd).

7.1.1.1-2.I1

Beskrivning återfinns i ITP.

7.1.1.1-3.I1

Observera att det alltid är försäkringsbolaget (eller annan kravställare) som godkänner säkerhetsprodukter (lås och larm)
Av försäkringsvillkoren framgår vilka krav man ställer för att försäkringen ska gälla fullt ut. Kontrollera alltid vilka krav som gäller innan du väljer att köpa och montera nya säkerhetsprodukter.

7.1.1.1-5.I1

Säkerhetsskåp skall uppfylla Stöldskyddsföreningens norm SS 3492.

7.1.1.1-6.I1

Nyckelschema är till hjälp där stora mängder nycklar hanteras och används för att enkelt se vilka nycklar som går vart. Kommer det exempelvis in en upphittad nyckel som man inte vet vart den går är det bara att knappa in den och söka fram vart den går förutsatt att den finns i ett nyckelsystem. Lika enkelt är det att ta fram vilka som har lånat nycklar som går till ett visst utrymme. Nyckelschema kan vara manuella eller ha datorstöd.

7.1.1.1-8.I1

I loggbok skall minst följande uppgifter noteras:
- besökares namn och organisation/företag
- beledsagares namn och organisatorisk tillhörighet
- tidpunkt för in- och utpassage
- syfte med besöket

7.1.1.1-9.I1

Skalskyddet kan innefatta larmade lokaler som under ej öppethållande är låsta.
Hur fönster skyddas måste också beaktas.
Datorer kan förses med vajerlås och förslagsvis låsas ihop parvis.
Via låsbart bleck eller motsvarande kan datorn förankras mot det underlag den står på.

7.2 Skydd av utrustning

7.2.1 Fysiskt skydd, elförsörjning och kablageskydd

Beroende av placering av utrustning krävs olika typer av fysiskt skydd.
Eventuella miljörisker skall speciellt beaktas.

7.2.1.1 *Anvisningar för placering och skydd av utrustning*

Pos	Text	Koppling till Instruktioner
Allmänt	Vad beträffar stöld av utrustning, speciellt datorutrustning, är inriktningen på ett starkt skalskydd, grundstenen för säkerhet.	
7.2.1.1-1	Brandskydd skall alltid finnas i eller i anslutning till server- och kommunikationsutrymme.	7.2.1.1-1.I1
7.2.1.1-2	Verksamhetskritisk information/material skall förvaras i säkerhetsskåp i låst utrymme.	7.2.1.1-2.I1
7.2.1.1-3	Reservutrustning skall förvaras i låst utrymme med begränsat tillträde.	---
7.2.1.1-4	Stöldbegärlig utrustning skall märkas på ett beständigt sätt.	7.2.1.1-4.I1
7.2.1.1-5	Placering av skrivare och faxutrustning styrs av den typ av information som hanteras.	7.2.1.1-5.I1

7.2.1.1-6	Bärbar utrustning skall, där så är möjligt, vara utrustade med wirelås vid arbete utanför ordinarie arbetsplats.	---

Instruktioner för placering och skydd av utrustning

7.2.1.1-1.I1

Kompletteras senare.

7.2.1.1-2.I1

Arkivering av information lagrad på datamedia skall ske i rum eller skåp som uppfyller Riksarkivets krav enligt RA-FS 1997:3.
Den norm som i första hand är aktuell heter EN 1047 (EU norm för brandklassning) där brandklass P = för pappersdokument och brandklass DIS = för olika typer av datamedia.

7.2.1.1-4.I1

Hänvisning till 5.1.1.1.

7.2.1.1-5.I1

Om känslig information skrivs ut skall möjligheten beaktas att använda utrustning som kräver exempelvis lösenord för att möjliggöra utskrift.

7.2.2 Säkerhet för utrustning utanför egna lokaler

Utrustning som används utanför egna lokaler skall skyddas så att samma säkerhetsnivå, som om den används i de egna lokalerna, uppnås.
Särskild hänsyn skall tas mot risk för stöld och informationsåtkomst.

7.2.2.1 *Anvisningar för distansarbetsplats*

Pos	Text	Koppling till Instruktioner
Allmänt	Det är allt vanligare att anställda arbetar utanför organisationens lokaler, i hemmet eller på annan plats. Dessa anvisningar avser arbete i hemmet med av staden tillhandahållen utrustning och kommunikationsförbindelse (=distansarbetsplats).	
7.2.2.1-1	Utrustning till distansarbetsplatsen skall väljas enligt stadens anvisningar för standardisering av datorer och liknande utrustning.	7.2.2.1-1.I1
7.2.2.1-2	Privat utrustning får inte användas.	---
7.2.2.1-3	Utrustning skall vara stöldskyddsmärkt på ett beständigt sätt.	7.2.2.1-3.I1
7.2.2.1-4	Aktiv skärmsläckare (5 minuter) med lösenord skall finnas.	---
7.2.2.1-5	Utrustning avsedd för distansarbete får endast användas av den anställde.	---
7.2.2.1-6	Information skall lagras på centralt angiven server.	---
7.2.2.1-7	Samma säkerhetsnivå avseende säkerhetsuppdateringar och virusskydd skall gälla för distansarbetsplatsen som för ordinarie arbetsplats.	7.2.2.1-7.I1
7.2.2.1-8	ISDN/ADSL kommunikation, tillhandahållen av staden, skall ske med hjälp av krypterat lösenordsutbyte mellan routrar.	---

Instruktioner för distansarbetsplats

7.2.2.1-1.I1

Detta beskrivs i ITP.

7.2.2.1-3.I1

Hänvisning till 5.1.1.1.

7.2.2.1-7.I1

Skyddet skall aktiveras automatiskt då datorn startas. Uppdatering av virusskyddet skall utföras automatiskt vid anslutning till stadens nätverk. Om detta ej är möjligt skall manuell uppdatering ske regelbundet.

7.2.2.2 *Anvisningar för mobil datoranvändning*

Pos	Text	Koppling till Instruktioner
Allmänt	I begreppet mobil datoranvändning innefattas användning av bärbara PC, handdatorer, avancerade mobiltelefoner och andra liknande enheter. För att få åtkomst till program och data krävs säkerhetsmässigt godtagbara lösningar.	
7.2.2.2-1	All uppringd analog kommunikation (modem) skall ske med hjälp av engångslösenord eller motsvarande.	7.2.2.2-1.I1
7.2.2.2-2	ISDN/ADSL kommunikation, VPN eller annan säker lösning skall ske med hjälp av krypterat lösenordsutbyte mellan routrar.	---
7.2.2.2-3	Uppkoppling mot stadens nätverk skall ske via ID-portalen.	7.2.2.2-3.I1
7.2.2.2-4	All lagrad information på intern minnesenhet skall krypteras såvida inte röjande av information medför allvarlig skada.	7.2.2.2-4.I1
7.2.2.2-5	Vid lagring på extern minnesenhet skall informationsinnehållet avgöra krypteringsbehovet.	---
7.2.2.2-6	För mobila enheter skall, om teknisk plattform stöder detta, antivirusskydd vara installerat och aktiverat.	7.2.2.2-6.I1
7.2.2.2-7	Aktiv skärmsläckare (5 minuter) skall finnas.	---
7.2.2.2-8	Bärbar utrustning skall skyddas med lösenord/motsvarande.	7.2.2.2-8.I1
7.2.2.2-9	Bärbar utrustning skall vara stöldskyddsmärkt på ett beständigt sätt.	7.2.2.2-9.I1
7.2.2.2-10	Före utlämning av handdator skall registrering och säkerhets-inställningar göras.	7.2.2.2-10.I1

Instruktioner för mobil datoranvändning

7.2.2.2-1.I1

Engångslösenord kan genereras antingen med hjälp av en dosa eller en s.k Soft Token, en programvara som kan installeras i mobiltelefon.

7.2.2.2-3.I1

Val av identifieringsätt styrs av aktuell säkerhetsprofil (via informationsklassificering).

7.2.2.2-4.I1

Av staden rekommenderad lösning (via tredje part) skall användas. Dock måste teknisk plattform beaktas så att störningar inte uppstår i verksamheten.

7.2.2.2-6.I1

Skyddet skall aktiveras automatiskt då enheten startas. Uppdatering av antivirusskyddet skall utföras automatiskt vid anslutning till stadens nätverk. Om detta ej är möjligt skall manuell uppdatering ske regelbundet.

7.2.2.2-8.I1

-Lösenordet skall innehålla minst 6 tecken.
-Lösenordet skall bestå av en blandning av alfanumeriska tecken.
-Användaren skall tvingas byta lösenord minst var 30:e dag,
-Lösenord skall ej kunna återanvändas.
-Lösenordet får ej medge "versionsuppdatering", ex.vis DEMO1, DEMO2 etc.
-Repeterbarhet av lösenord skall vara förhindrat i minst 13 generationer.
-Låsning av användare p.g.a inaktivitet skall ske efter 60 dagar där så medges.
-Maximalt tre felaktiga försök till inloggning skall vara tillåtet. Därefter låses användaridentiteten.

7.2.2.2-9.I1

Hänvisning till 5.1.1.1.

7.2.2.2-10.I1

Kompletteras senare.

7.2.3 Avveckling/återanvändning av utrustning

Avveckling/återanvändning av utrustning som innehåller lagrad information skall ske så att obehörig informationsåtkomst förhindras.

7.2.3.1 *Anvisningar för avveckling/återanvändning av utrustning*

Pos	Text	Koppling till Instruktioner
Allmänt	Det är viktigt att gällande regelverk följs så att oönskad informationsåtkomst förhindras.	
7.2.3.1-1	Vid avyttring av datamedia med känsligt innehåll skall åtgärder vidtas så att informationsinnehållet görs oläsbart.	7.2.3.1-1.I1

Instruktioner för avveckling/återanvändning av utrustning

7.2.3.1-1.I1

Datamedia skall raderas och överskrivas eller destrueras mekaniskt på ett säkert sätt.

Destruktionen dokumenteras på blankett 'Anmälan avyttring av datamedia' eller på motsvarande sätt. Av dokumentationen skall framgå datum och till vem datamediet har lämnats för destruktion. Destruktionsintyg från destruktionsfirman eller leverantören som återtagit utrustningen skall arkiveras av respektive tekniskt ansvarig.

7.3 Allmänna åtgärder

7.3.1 Publika miljöer

Skalskydd skall anordnas med särskilt beaktande av den publika miljön.
Åtgärder skall vidtas för att motverka anonym användning av datorer som staden upplåter publikt.

7.3.1.1 *Anvisningar för datorer i publik miljö*

Pos	Text	Koppling till Instruktioner
Allmänt	De publika miljöer (medborgarkontor, bibliotek, skolor etc) som staden tillhandahåller för medborgarna har oftast IT-utrustning för informationssökning/-hantering.	
7.3.1.1-1	För särskilt utsatta arbetsplatser skall utrustning vara fastlåst.	---
7.3.1.1-2	I publika miljöer där datorer tillhandahålls skall inre och yttre skalskydd beaktas.	7.3.1.1-2.I1
7.3.1.1-3	I publika miljöer där datorer tillhandahålls och ingen åtkomstbegränsning är uppsatt skall lånekort, tidbokningslista eller motsvarande användas för att motverka anonym användning.	7.3.1.1-3.I1
7.3.1.1-4	Endast publika tillämpningar skall kunna nås från datorn.	---
7.3.1.1-5	Möjlighet skall finnas att förhindra åtkomst till webbsidor/-adresser (URL) med olämpligt innehåll och/eller skadlig påverkan.	7.3.1.1-5.I1

Instruktioner för datorer i publik miljö

7.3.1.1-2.I1

Hänvisning till 7.1.1.1

7.3.1.1-3.I1

Stadsbibliotekets system för utlåning används vid ett flertal förvaltningar. Lånekorten fungerar då som garanti för identiteten då dessa endast får hämtas mot uppvisande av legitimation.
Utöver denna metod kan egna användarlistor upprättas på enkelt vis som görs vid de flesta Medborgarkontor. Det väsentliga är att ingen anonym användning förekommer.

7.3.1.1-5.I1

Filter mot surfning till olämpliga sidor kan beställas som tjänst av stadens outsourcingpartners. Stadens informationssäkerhetschef kan bistå med ytterligare stöd.

8 Styrning av kommunikation och drift

Gjord informationsklassificering styr säkerhetskraven för ledning och drift av IT-system och kommunikationsutrustning.

8.1 Driftrutiner och driftansvar

8.1.1 Dokumenterade driftrutiner

Driftrutiner skall vara dokumenterade och hållas aktuella. Ändringsrutin för driftdokumentation skall tillämpas.

I drift- och/eller förvaltningsåtagande för IT-system skall anvisningar finnas för att regelbundet kunna ta del av leverantörers systemrevisioner. Samtliga uppdateringar skall värderas utifrån ett säkerhetsperspektiv och de uppdateringar som innebär minskning av riskkostnaden skall införas.

8.1.1.1 *Anvisningar för informationsklassificering*

Hänvisning till 5.2.1.1.

8.1.1.2 *Anvisningar för driftdokumentation*

Pos	Text	Koppling till Instruktioner
Allmänt	För att kunna garantera överenskommet IT-stöd krävs en god ordning och aktualitet gällande driftdokumentation.	
8.1.1.2-1	Originaldokumentation skall placeras i dokumentskåp.	8.1.1.2-1.I1
8.1.1.2-2	Driftdokumentation skall hållas aktuell och vara godkänd av tekniskt systemansvarig.	---
8.1.1.2-3	Det skall finnas en förteckning över all utrustning och programvara.	8.1.1.2-3.I1 8.1.1.2-3.I2

Instruktioner för driftdokumentation

8.1.1.2-1.I1

Arkivering av information lagrad på datamedia skall ske i rum eller skåp som uppfyller Riksarkivets krav enligt RA-FS 1997:3.
Den norm som i första hand är aktuell för dokumentskåp heter EN 1047 (EU norm för brandklassning) där brandklass P = för pappersdokument och brandklass DIS = för olika typer av datamedia.
Dokumentskåp skall uppfylla Brandklass 90 P, godkänt av Statens Provningsanstalt.

8.1.1.2-3.I1

Hänvisning till 5.1.1.1.

8.1.1.2-3.I2

Hänvisning till 5.1.1.1.

8.1.1.3 *Anvisningar för säkerhetsuppdateringar (patchar)*

Pos	Text	Koppling till Instruktioner
Allmänt	Säkerhetsuppdateringar skall alltid bedömas innan aktuell patch kan installeras.	
8.1.1.3-1	Rutin skall finnas för att hantera leverantörs säkerhetsuppdateringar.	8.1.1.3-1.I1

Instruktioner för säkerhetsuppdateringar (patchar)

8.1.1.3-1.I1

Samtliga servrar skall inom 24 timmar efter utgivning av ny virussignaturfil ha denna installerad.

Utgivna, viktiga säkerhetspatchar skall, inom 7 dygn, vara testade och installerade.

8.1.2 Styrning av ändringar i driftmiljö

Förändringar i driftmiljö, utrustning och rutiner skall styras via befintliga anvisningar, ex.vis

- identifiering och registrering av större ändringar;
- konsekvensanalys av sådana ändringar;
- godkännande/beslutsform för ändringar;
- informationskrav till verksamheten;
- rutin för avbrytande av och återställande av misslyckade ändringar.

Fastställda processer för hantering av förändringar i IT-system skall alltid följas.

Process för ändringshantering skall följas även för åtgärder som är av rent infrastrukturell karaktär. Motsvarande process skall följas när det gäller IT-system som anskaffas från extern leverantör.

Samtliga ändringar skall kunna härledas till en ansvarig beställare.

8.1.2.1 *Anvisningar för ändringar i driftmiljö*

Pos	Text	Koppling till Instruktioner
Allmänt	Rutiner för ändringshantering minskar riskerna för driftstörningar.	
8.1.2.1-1	Rutin för ändringshantering (även för mindre ändringar) skall finnas etablerad inom systemets förvaltningsorganisation.	8.1.2.1-1.I1
8.1.2.1-2	Samtliga ändringar skall kunna härledas till en beställare.	---
8.1.2.1-3	All ändring av programvara skall godkännas innan installation i utbildnings-/produktionsmiljö.	8.1.2.1-3.I1

Instruktioner för ändringar i driftmiljö

8.1.2.1-1.I1

Respektive systemägarrepresentant, såväl central som lokal, ansvarar för detta i samråd med driftteknisk personal.

8.1.2.1-3.I1

Innan installation i produktionsmiljö skall det finnas ett testprotokoll, undertecknat av systemägarrepresentant eller annan av honom/henne utsedd person.

IT-handboken, del Testhandboken skall följas.

8.2 Driftgodkännande och planering

8.2.1 Driftgodkännande

Driftgodkännande skall föregås av en definierad testfas.

8.2.1.1 *Anvisningar för driftgodkännande och planering*

Pos	Text	Koppling till Instruktioner
Allmänt	Innan driftsättning skall identifierade säkerhetskrav vara omhändertagna.	
8.2.1.1-1	Systemet skall vara driftgodkänt av systemägarrepresentanten.	8.2.1.1-1.I1
8.2.1.1-2	Acceptanstest skall vara utförd före driftöverlämning.	8.2.1.1-2.I1
8.2.1.1-3	SLA ingående i Drift- och förvaltningsavtal skall vara fastställt och kommunicerat till berörda parter.	---
8.2.1.1-4	Kapacitetsbehov/prestanda av lagringsutrymme, processorer etc skall följas upp för eventuella anskaffningsbehov.	8.2.1.1-4.I1

Instruktioner för driftgodkännande och planering

8.2.1.1-1.I1

En del i driftgodkännandet innefattar att informationsklassificering typ B (enligt HKL) skall vara genomförd. Generellt hänvisas till IT-handboken.

8.2.1.1-2.I1

Systemanpassad checklista skall användas så att beställaren via test/kontroll fastställer att det som levereras är det som beställts. Generellt hänvisas till IT-handboken.

8.2.1.1-4.I1

Kontroll av filtyper, filstorlekar och liknande tekniska uppgifter skall utföras av tekniskt driftansvarig, med stickprov eller vid behov.

8.3 Skadliga program

8.3.1 Skydd mot skadliga program

Användare skall vara medvetna om att datorer skall användas i enlighet med verksamhetens syfte och fastställda anvisningar.

8.3.1.1 *Anvisningar för åtgärder mot skadliga program*

Pos	Text	Koppling till Instruktioner
Allmänt	Skadliga program (virus, maskar, logiska bomber, trojaner, spyware etc) innehåller kod som har till syfte att negativt påverka datorer, kommunikation och information.	
8.3.1.1-1	Antivirusprogram skall installeras och kontinuerligt uppdateras på stadens datorer.	8.3.1.1-1.I1
8.3.1.1-2	Programvara som installeras i stadens datorer skall vara godkänd av aktuell IT-chef eller motsvarande.	---
8.3.1.1-3	Nedladdning/lagring av programvaror och filer från okända eller tvivelaktiga webplatser är inte tillåtet.	---

Instruktioner för åtgärder mot skadliga program

8.3.1.1-1.I1

Alla stadens datorer, servrar och klienter, skall vara skyddade mot skadlig kod/skadliga program. Centralt avtalade produkter skall i möjligaste mån användas. Processen för att nyttja dessa hanteras av SLK, IT-infrastrukturenheten.
Skyddet skall aktiveras automatiskt då datorn startas. Uppdatering av antivirusskyddet skall utföras automatiskt vid anslutning till stadens nätverk. Om detta ej är möjligt skall manuell uppdatering ske regelbundet.

8.4 Ordning och reda

8.4.1 Säkerhetskopiering

Utrymme där säkerhetskopior eller skåp som innehåller säkerhetskopior förvaras skall brandskyddas i enlighet med gällande lagstiftning samt eventuella normer från försäkringsinstitut.
Kritiska säkerhetsfunktioner som återställning av säkerhetskopior skall övas och kontrolleras.

8.4.1.1 *Anvisningar för säkerhetskopiering*

Pos	Text	Koppling till Instruktioner
Allmänt	Anvisningarna omfattar hur lagringsmedia hanteras, lagras och märks.	
8.4.1.1-1	Säkerhetskopiering skall ske enligt vad som överenskommits i SLA/drift- och förvaltningsavtal.	8.4.1.1-1.I1
8.4.1.1-2	Datamediaskåp eller motsvarande utrymme skall användas för förvaring av datamedia.	8.4.1.1-2.I1

Instruktioner för säkerhetskopiering

8.4.1.1-1.I1

Respektive systemägarrepresentant fastställer krav på frekvens av säkerhetskopiering, förvaringsplats för arkivkopia, krav på återläsningstid o.s.v i SLA.

8.4.1.1-2.I1

Arkivering av information lagrad på datamedia skall ske i rum eller skåp som uppfyller Riksarkivets krav enligt RA-FS 1997:3.
Den norm som i första hand är aktuell heter EN 1047 (EU norm för brandklassning) där brandklass P = för pappersdokument och brandklass DIS = för olika typer av datamedia. Datamediaskåp skall uppfylla Brandklass 90 P, godkänt av Statens Provningsanstalt.

8.4.2 Loggar

Kritiska händelser i drift och datakommunikation skall vara spårbara. Detta bör i första hand åstadkommas med automatiska loggningsfunktioner. Alternativt redovisas händelser skriftligt.
Loggning bör inriktas på drift-, transaktions- och säkerhetshändelser.

8.4.2.1 *Anvisningar för logghantering*

Pos	Text	Koppling till Instruk-tioner
Allmänt	Behovet av loggning och uppföljning av loggar (analys) fastställs av systemägarrepresentanten i enlighet med verksamhetens behov samt genomförd klassificering.	
8.4.2.1-1	Loggning och analys avseende obehöriga åt-komstförsök till informationstillgångar (nätverk, information mm) skall genomföras regelbundet oavsett klassificeringsresultat.	8.4.2.1-1.I1
8.4.2.1-2	Loggar skall finnas så att aktiviteter utförda av personer med hög behörighet kan spåras vid behov.	8.4.2.1-2.I1

Instruktioner för logghantering

8.4.2.1-1.I1
Generering och sparande av loggar är avhängigt teknisk plattform. Vissa analys-verktyg kommer att tillhandahållas av Stadsledningskontoret, IT-infrastrukturenheten.

8.4.2.1-2.I1
Analysverktyg kommer att tillhandahållas av Stadsledningskontoret, IT-infrastrukturenheten.

8.5 *Styrning av nätverk*

8.5.1 Nätverk

Anvisningar och instruktioner skall finnas för att uppnå och vidmakthålla fastställd säkerhetsnivå i stadens nätverk.

8.5.1.1 *Anvisningar för säkerhetsuppdateringar (patchar)*

Hänvisning till 8.1.1.3.

8.5.1.2 *Anvisningar för säkerhetsarkitektur nätverk*

Pos	Text	Koppling till Instruktioner
Allmänt	Speciell hänsyn krävs vid kommunikation över organisationsgränser samt vid överfö-ring av känslig information.	
8.5.1.2-1	Information skall kunna överföras oförvans-kad i nätverk.	8.5.1.2-1.I1
8.5.1.2-2	Organisationens nätverk skall följa gällande säkerhetsstruktur.	8.5.1.2-2.I1
8.5.1.2-3	Vid trådlös kommunikation skall gällande säkerhetsarkitektur följas.	8.5.1.2-3.I1
8.5.1.2-4	All extern (riktad till egen organisation) trafik baserad på TCP/IP skall gå via brand-vägg och filtreras utifrån verksamhetsbeho-ven.	8.5.1.2-4.I1

Instruktioner för säkerhetsarkitektur nätverk

8.5.1.2-1.I1
Hänvisning till ITP, kapitel Teknisk IT-säkerhet.

8.5.1.2-2.I1

Hänvisning till ITP, kapitel Teknisk IT-säkerhet.

8.5.1.2-3.I1

Bedömning skall göras om det är möjligt att uppnå samma effekt med ett trådbaserat nät.
Säkerhetsarkitekturen är uppbyggd av nedanstående punkter:

- WLAN skall alltid anslutas via brandvägg
- Autenticering skall alltid ske med certifikat eller engångslösenord
- Kontroller och penetrationstester skall ske regelbundet
- Nätverksnamnet skall inte annonseras via accesspunkten (AP)
- Nätverksnamnet skall inte anknyta till verksamheten
- Accesspunkterna skall vara skalskyddade
- Access till Internet skall ej kunna ske utan inloggning
- IP-adresser via DHCP skall endast utdelas till kända klienter
- Information som kan bedömas som sekretessbelagd skall ej hanteras via WLAN utan kryptering.

8.5.1.2-4.I1

Generellt skall oönskad trafik vara spärrad.
Följande grundfunktioner bör finnas i en brandvägg:

- Paketfiltering (TCP/UDP portar, ip-adresser)
- Tillståndsbaserad filtrering (autenticering)
- NAT
- Fjärrstyrning
- VPN funktionalitet
- VLAN hantering
- Övervakning av trafik (loggar)

Det är viktigt att regelverk finns gällande porthantering. Hänsyn måste tas till om det gäller åtkomst till stadens gemensamma resurser alternativt egen förvaltning/bolag/skola och vem som vill nå aktuell resurs (behörighetsaspekt).
I regelverket skall återfinnas roller/ansvar och rutiner för porthantering.

8.6 Mediahantering och mediasäkerhet

8.6.1 Avveckling av media

Lagringsmedia skall avvecklas på säkert sätt när de inte längre behövs.
Följande skall särskilt beaktas:
- lagringsmedia som innehåller känslig information destrueras alternativt raderas på ett säkert sätt
- av spårbarhetsskäl skall det dokumenteras hur känsligt material avvecklas.

8.6.1.1 *Anvisningar för avveckling av media*

Pos	Text	Koppling till Instruktioner
Allmänt	Det är viktigt att förhindra att lagrad information (ej programvara/motsvarande) kan användas i oönskat syfte.	
8.6.1.1-1	Lagringsmedia från driftmiljö (dvs ej enskild användare) som ej längre skall användas i egen organisation skall förtecknas för att bibehålla spårbarhet.	8.6.1.1-1.I1

8.6.1.1-2	Vid avyttring av lagringsmedia med känsligt innehåll skall åtgärder vidtas så att informationsinnehållet görs oläsbart.	8.6.1.1-2.I1

Instruktioner för avveckling av media

8.6.1.1-1.I1
Register skall upprättas för all typ av media (band, disk etc) som ej längre används. Även förvaringsplats /destination skall anges. Avyttring skall dokumenteras. Av dokumentationen skall framgå avyttringsdatum, typ av information och till vem lagringsmediet har lämnats.

8.6.1.1-2.I1
Lagringsmedia skall raderas och överskrivas eller destrueras mekaniskt på ett säkert sätt. Destruktionen skall dokumenteras. Av dokumentationen skall framgå avyttringsdatum, typ av information och till vem lagringsmediet har lämnats för destruktion. Destruktionsintyg från destruktionsfirman eller leverantören som återtagit utrustningen skall arkiveras av teknisk systemförvaltare.

8.6.2 Säkerhet för systemdokumentation

Systemdokumentation skall skyddas i enlighet med aktuell säkerhetsprofil.

8.6.2.1 *Anvisningar för systemdokumentation*

Pos	Text	Koppling till Instruktioner
Allmänt	Systemdokumentation skall skyddas i enlighet med den klassificering som gäller för aktuellt system.	
8.6.2.1-1	Systemdokumentation skall hållas aktuell och vara godkänd av systemförvaltare.	---

8.7 Utbyte av information och program

8.7.1 Säkerhet i elektronisk handel

Regleras i avtal mellan berörda parter.

8.7.1.1 *Anvisningar för elektronisk handel*

Pos	Text	Koppling till Instruktioner
Allmänt	Teknik för elektronisk sigill skall användas för att säkerställa att information inte förvanskas. Elektronisk signatur är ett sätt att visa att författaren till ett elektroniskt dokument är den han utger sig för att vara.	
8.7.1.1-1	Vid betalningsförmedling/motsv. skall elektroniskt sigill/certifikat användas.	8.7.1.1-1.I1

8.7.1.1-2	Elektronisk signering skall användas då det är juridiskt viktigt att kunna knyta en person till ett visst dokument. Teknikval avgörs via informationsklassificering.	8.7.1.1-2.I1

Instruktioner för elektronisk handel

8.7.1.1-1.I1

Stadens standard för elektroniskt sigill skall användas. Redovisningsstaben på Stadsledningskontoret kan kontaktas i frågan.

8.7.1.1-2.I1

Kompletteras när behov av elektronisk signering aktualiseras.

8.7.2 Säkerhet i elektroniskt offentliggjord information

Åtgärder skall vidtas för att skydda riktigheten hos elektroniskt offentliggjord information.

8.7.2.1 *Anvisningar för elektroniskt offentliggjord information*

Pos	Text	Koppling till Instruktioner
Allmänt	Åtgärder skall vidtas för att skydda riktigheten hos elektroniskt offentliggjord information.	
8.7.2.1-1	Det skall finnas en formell process för godkännande innan information görs allmänt tillgänglig.	8.7.2.1-1.I1
8.7.2.1-2	All publicering skall ske via en testmiljö, så kallad staging.	---

Instruktioner för elektroniskt offentliggjord information

8.7.2.1-1.I1

Ansvarig utgivare för WEB-sidor måste alltid finnas. Denne ansvarar för att erforderliga rutiner upprättas och efterlevs.

8.7.3 Annat informationsutbyte

Anvisningar skall finnas för att skydda informationsutbyte vid användning av röst-, fax- och videokommunikationsutrustning.

8.7.3.1 *Anvisningar för annat informationsutbyte*

Pos	Text	Koppling till Instruktioner
Allmänt	Information kan exponeras för obehörig genom brist på medvetenhet, policy eller anvisningar gällande röst-, fax- och videokommunikationsutrustning.	
8.7.3.1-1	Telefonsamtal med känslig information skall ske i ej avlyssningsbar miljö.	---
8.7.3.1-2	Känslig information på whiteboard, bläderblock och motsvarande skall avlägsnas/förstöras efter avslutat möte/motsv.	---

8.7.3.1-3	Vid användning av faxutrustning i samband med känslig information skall aktuell instruktion följas.	8.7.3.1-3.I1

Instruktioner för elektroniskt offentliggjord information

8.7.3.1-3.I1
Om känslig information skall hanteras via fax skall krypterad fax användas. Som ett alternativ kan fax med accesskontroll (PIN-kod eller motsvarande) användas.

9 Styrning av åtkomst

Åtkomst till IT-system och nätverk skall styras utifrån verksamhetsbehov och säkerhetskrav.

9.1 Verksamhetskrav på styrning av åtkomst

Genomförd informationsklassificering avgör åtkomst till information.

9.2 Styrning av användares åtkomst

9.2.1 Behörighetsadministration

Hantering av behörigheter skall ske enligt gällande anvisningar.

9.2.1.1 *Anvisningar för hantering av behörighetsadministration*

Pos	Text	Koppling till Instruktioner
Allmänt	Enbart den som, för att kunna utföra sina arbetsuppgifter, har behov av åtkomst till informationstillgångar skall tilldelas åtkomsträttigheter (behörigheter).	
9.2.1.1-1	Behörighetsadministratörer skall finnas utsedda för stadens IT-system.	---
9.2.1.1-2	Instruktioner för hantering av behörigheter skall finnas.	9.2.1.1-2.I1
9.2.1.1-3	Med lämpligt tidsintervall skall listor på samtliga behörigheter ta ut och kontrolleras. Intervallet avgörs av omfattningen på förändringar..	---
9.2.1.1-4	Behörighetsadministratör skall omgående meddelas då personal slutar sin anställning eller annan förändring sker som påverkar behörigheten.	---
9.2.1.1-5	För vikarier och inhyrd personal skall tilldelning av behörigheter ske enligt separata instruktioner.	9.2.1.1-5.I1
9.2.1.1-6	Tilldelning av behörigheter till personer med kommuncentrala arbetsuppgifter sker enligt systemägarrepresentantens instruktioner.	---

Instruktioner för hantering av behörighetsadministration

9.2.1.1-2.I1
Verksamhetschef beslutar om aktuell behörighet.

För tilldelning av behörigheter i centrala system gäller:
Beställning, signerad av verksamhetschef, med specificerade åtkomstkrav skall sändas till lokal behörighetsadministratör. Beställningen sänds sedan till den som är ansvarig för respektive behörighetskontrollsystem (vanligen driftleverantör).
Driftleverantören ombesörjer uppläggning av identitet i det övergripande behörighets-kontrollsystemet enligt beställningen. Övriga önskemål (till system i stordatormiljö) sänds till utsedda behörighetsadministratörer för J90 och BRA.

För tilldelning av behörigheter i lokala nätverk och system gäller:
Beställning, signerad av aktuell verksamhetschef, av behörigheter till nätverk och system skall sändas till lokala IT-enheten på förvaltningen/bolaget. Denna ombesörjer att uppläggning av användare och tilldelning av behörigheter sker. Om annan förvaltning eller bolag skulle påverkas måste dessa underrättas omgående.

För tilldelning av behörigheter utanför den egna förvaltningen gäller:
Vid behörighetstilldelning utanför egen förvaltning sänds beställning, efter signering av verksamhetschef, till systemförvaltare för aktuellt system. Denne stämmer av beställningen med systemägarrepresentanten och ombesörjer att behörighet tilldelas enligt ordinarie rutiner samt svarar även för att behörigheten avslutas efter ändring av befattnings- eller anställningsförhållanden eller motsvarande. På ansökan om behörighet skall därför alltid giltighetstid anges.
Om informationsägare är annan än systemägaren skall denna underrättas, exempelvis genom epost.

9.2.1.1-5.I1

På de arbetsplatser där inhyrd personal anlitas skall finnas ett antal behörigheter, förvarade i slutna kuvert och inlåsta. Identiteten för dessa behörigheter skall vara så konstruerad att den anger aktuell arbetsplats. Ansvarig arbetsledare skall ha rätt att tilldela en sådan behörighet.
Då det gäller nivå och omfattning för dessa behörigheter skall de, i samråd mellan systemförvaltare och arbetsledare vid respektive arbetsplats, utformas så att behörigheten gör det möjligt för vederbörande att utföra ålagda uppgifter men ingenting mer. Antalet varianter av behörighet vid en viss arbetsplats skall vara så lågt som möjligt, helst endast en nivå, så att administrationen blir så enkel som möjligt.
För dessa specialkonstruerade vikariatsbehörigheter skall följande krav gälla:
- de skall endast ge möjlighet att nå och rätt att arbeta i aktuell tillämpning
- de skall endast gälla inom den del av organisationen, som uppdraget avser
- lösenorden (i nät och tillämpning) skall omgående bytas då vikariatet går ut
- byte av lösenord skall göras av berörd chef/arbetsledare alternativt systemförvaltare
- id och lösenord skall då de ej används förvaras på ett betryggande sätt (kassaskåp eller motsvarande)

För att uppfylla stadens krav på att varje transaktion skall kunna knytas till den som utfört den, måste dessa i grunden anonyma behörigheter kompletteras med en manuell användarlogg. Den består helt enkelt av en lista i vilken arbetsledaren antecknar att en viss behörighet använts av vikarie X under en viss tid. Vikarien skall också kvittera ut behörigheten i denna logg. Loggen skall förvaras under lås på samma sätt som kuverten med behörigheterna. Då vikariatet upphör skall arbetsledaren snarast ombesörja att lösenordet byts och att behörigheten på nytt läggs i ett slutet kuvert i ett låst utrymme till vilket få personer har tillträde. Genom den manuella loggen blir det möjligt att i efterhand fastställa vem som vid en viss tidpunkt varit innehavare av en viss behörighet.

9.2.2 Behörighetskontroll

För användare skall åtkomst till informationstillgångar ske via behörighetskontrollsystem där användaren har en unik identitet och lösenord eller eventuellt en rolltillhörighet.

9.2.2.1 *Anvisningar för behörighetskontroll*

Pos	Text	Koppling till Instruktioner
Allmänt	Behörighetskontrollsystem (BKS) skall finnas och vara integrerade i de plattformar som väljs för serveroperativsystem, databashanterare och tillämpningar.	
9.2.2.1-1	Lösenord skall generellt vara individuella och får ej överlåtas eller lånas ut.	9.2.2.1-1.I1
9.2.2.1-2	Lösenord skall skapas enligt gällande instruktioner.	9.2.2.1-2.I1
9.2.2.1-3	Som alternativ till lösenord kan biometrisk igenkänning användas.	9.2.2.1-3.I1
9.2.2.1-4	Som alternativ till lösenord kan elektroniskt id-kort användas.	9.2.2.1-4.I1
9.2.2.1-5	I publika miljöer där datorer tillhandahålls skall lånekort, tidbokningslista eller motsvarande användas för att motverka anonym användning.	9.2.2.1-5.I1

Instruktioner för behörighetskontroll

9.2.2.1-1.I1

BKS skall vara integrerade i de plattformar som väljs för serveroperativsystem, databashanterare och tillämpningar.

Undantag från den generella regeln kan förekomma men skall alltid hanteras i samråd med stadens informationssäkerhetschef. Dock skall alltid möjlighet till spårbarhet finnas.

9.2.2.1-2.I1

-Lösenordet skall innehålla minst 6 tecken.
-Lösenordet skall bestå av en blandning av alfanumeriska tecken.
-Användaren skall tvingas byta lösenord minst var 30:e dag,
-Lösenord skall ej kunna återanvändas.
-Lösenordet får ej medge ”versionsuppdatering”, ex.vis DEMO1, DEMO2 etc.
-Repeterbarhet av lösenord skall vara förhindrat i minst 13 generationer.
-Låsning av användare p.g.a inaktivitet skall ske efter 60 dagar där så medges.
-Maximalt tre felaktiga försök till inloggning skall vara tillåtet. Därefter låses användaridentiteten.

9.2.2.1-3.I1

Biometriska metoder, t.ex fingermönsteravläsning används idag främst inom grundskolor i Stockholm. För information och installationshjälp, kontakta IT-infrastrukturenheten, Stadsledningskontoret.

9.2.2.1-4.I1

Inom staden finns flera elektroniska tjänster som bygger på att man identifierar sig med sitt elektroniska ID-kort. En av dessa är eSkrivbordet, (som i sin tur innehåller ett antal tillämpningar t.ex Groupwise och Office). Inom kort kommer också

möjligheten att tillämpa så kallad Single Sign-On vilket innebär att man bara gör en påloggning och får tillgång till flera system.
För ytterligare information se dokumentet Elektroniska ID-kort i Stockholms stad [länk].

9.2.2.1-5.I1

Hänvisning till 7.3.1.1.

9.3 Styrning av åtkomst till nätverk

9.3.1 Utnyttjande av nätverkstjänster

Rättighet att utnyttja olika former av nätverkstjänster skall beslutas och tilldelas enligt samma principer som åtkomststyrning i övrigt.

9.3.1.1 *Anvisningar för nätverksanslutning*

Pos	Text	Koppling till Instruktioner
Allmänt	Datakommunikation är en fundamental och kritisk resurs som kräver speciell fokus ur säkerhetssynpunkt. I ITP finns närmare beskrivet vad som gäller för anslutning till stadens nätverk.	
9.3.1.1-1	Inga modem får anslutas till persondatorer i stadens nät.	---
9.3.1.1-2	All extern kommunikation mot stadens nätverk skall ske via ID-portalen, modempoolen eller VPN-lösning i speciella fall.	9.3.1.1-2.I1
9.3.1.1-3	All extern trafik (riktad till egen organisation) baserad på TCP/IP skall gå via brandvägg och filtreras utifrån verksamhetsbehov.	9.3.1.1-3.I1
9.3.1.1-4	För servicetjänster on-line skall avtal finnas med den part som har tillstånd till uppkopplingen.	---
9.3.1.1-5	Till stadens nätverk får inga andra än av staden, för ändamålet, konfigurerade datorer anslutas.	9.3.1.1-5.I1
9.3.1.1-6	Användning av trådlösa nätverk (WLAN) skall ske med stor restriktivitet och baserat på verksamhetsbehov.	9.3.1.1-6.I1

Instruktioner för nätverksanslutning

9.3.1.1-2.I1

Val av identifieringsätt styrs av aktuell säkerhetsprofil (via informationsklassificering).

9.3.1.1-3.I1

Hänvisning till 8.5.1.2.

9.3.1.1-5.I1

Konsulters och andra leverantörers utrustning får dock anslutas till stadens nätverk med systemägarepresentants/motsvarande tillstånd.

9.3.1.1-6.I1

Hänvisning till 8.5.1.2.

9.4 Styrning av åtkomst till operativsystem

9.4.1 Åtkomst till operativsystem

Systemadministratörer skall kunna identifieras och styras vad avser åtkomst till operativsystem.

9.4.1.1 *Anvisningar för åtkomst till operativsystem*

Pos	Text	Koppling till Instruktioner
Allmänt	Restriktivitet skall gälla vid tilldelning av åtkomsträttigheter till operativsystem.	
9.4.1.1-1	Operatörskonsolfunktion skall skyddas med stark identifiering.	9.4.1.1-1.I1
9.4.1.1-2	Max 3 inloggningsförsök skall tillåtas. Därefter spärras användarkontot.	

Instruktioner för åtkomst till operativsystem

9.4.1.1-1.I1

Åtkomst till konsol skall skyddas med antingen komplexa lösenord (10 tecken, blandning av gemener, versaler och siffror), certifikat eller engångslösenord.

9.5 Styrning av åtkomst till tillämpningar

9.5.1 Åtkomst till tillämpningar

Säkerhetsåtgärder skall vidtas för att styra åtkomst till tillämpningar.

9.5.1.1 *Anvisningar för åtkomst till databaser/information*

Pos	Text	Koppling till Instruktioner
Allmänt	Anvisningarna syftar till att minska riskerna för obehörig åtkomst av information i IT-system.	
9.5.1.1-1	Systemägarrepresentant skall besluta om ett IT-systems information skall vara åtkomlig från externa platser.	---
9.5.1.1-2	Alla användare som skapar eller tillför information i IT-system skall använda personliga användarkonton.	---
9.5.1.1-3	Max 3 inloggningsförsök skall tillåtas. Därefter spärras användarkontot.	---
9.5.1.1-4	SQL-, ODBC-, ADO [**A**ctiveX **D**ata **O**bjects] -tjänster (m.fl.) får inte installeras så att IT-systemets databas kan anropas från klient utan att åtkomst prövas av tillämpade behörighetskontrollfunktioner.	---
9.5.1.1-5	Rutin skall finnas för utlämnande av allmän handling där information erhålls från IT-system.	9.5.1.1-5.I1

Instruktioner för åtkomst till databaser/information

9.5.1.1-5.I1

Utlämnandet kan ske på följande sätt: Antingen genom utskrift, digitalkopia eller på bildskärm, exempelvis presentationsterminal. Allmänheten kan begära att få använda en terminal om fyra förutsättningar är uppfyllda:

1. Användandet skall inte ge någon möjlighet att komma åt handlingar som inte är allmänna.
2. Det skall inte heller vara möjligt att komma åt sekretessbelagda handlingar.
3. Det skall inte finnas någon risk att handlingarna förstörs eller förvanskas.
4. Det skall inte hindra det ordinarie arbetet.

9.5.1.2 *Anvisningar för kryptering*

Pos	Text	Koppling till Instruktioner
Allmänt	Behovet av kryptering skall beaktas och styras av informationens värde.	
9.5.1.2-1	Rekommenderade metoder för kryptering skall användas.	9.5.1.2-1.I1

Instruktioner för kryptering

9.5.1.2-1.I1
Beskrivning av, av staden rekommenderade, metoder återfinns i ITP.

9.6 Övervakning av systemåtkomst och systemanvändning

9.6.1 Loggning av händelser

Loggar som registrerar avvikelser och andra säkerhetsrelevanta händelser skall föras och bevaras under fastställd tid.

9.6.1.1 *Anvisningar för logghantering*

Hänvisning till 8.4.2.1.

9.7 Mobil datoranvändning och distansarbete

9.7.1 Mobil datoranvändning

Den ökade säkerhetsrisk som föreligger vid mobil datoranvändning skall beaktas i Anvisningar och Instruktioner.

9.7.1.1 *Anvisningar för mobil datoranvändning*

Hänvisning till 7.2.2.2.

9.7.2 Distansarbete

Samma säkerhetsnivå skall gälla för distansarbetsplats som för ordinarie arbetsplats.

9.7.2.1 *Anvisningar för distansarbetsplats*

Hänvisning till 7.2.2.1.

10 Systemutveckling/-anskaffning och systemunderhåll

Systemutveckling skall alltid bedrivas i enlighet med fastställda modeller och metoder. För samtliga informationstillgångar skall säkerhetskrav sammanställas med genomförd riskanalys och informationsklassificering enligt kapitel 5.2 som grund.

10.1 Säkerhetskrav på IT-system

10.1.1 Analys och specifikation av säkerhetskrav

Säkerhetskrav skall vara åtgärdade innan driftgodkännande kan ges.

10.1.1.1 *Anvisningar för driftgodkännande och planering*

Hänvisning till 8.2.1.1.

10.1.1.2 *Anvisningar för informationsklassificering*

Hänvisning till 5.2.1.1.

10.2 Säkerhet i tillämpningar

10.2.1 Informationskvalitet

Kontrollmekanismer skall finnas så att förväntad informationskvalitet garanteras.

10.2.1.1 *Anvisningar för användardokumentation*

Pos	Text	Koppling till Instruktioner
Allmänt	Användardokumentation utformas med hänsyn till olika användarens kunskaper och behov och riktas både till erfarna användare och till nybörjare.	
10.2.1.1-1	Användardokumentation skall finnas tillgänglig för alla användare.	---
10.2.1.1-2	Som alternativ/komplement skall användardokumentationen finnas tillgänglig 'online'.	---

10.2.1.2 *Anvisningar för informationssäkerhet vid utveckling och tillämpning av Internettjänster*

Pos	Text	Koppling till Instruktioner
Allmänt	I samband med utveckling av nya tillämpningar och/eller förändring bör möjligheten till användande av elektronisk identifiering prövas. Elektronisk id stöder framför allt tre huvudfunktioner: stark autenticering (säker inloggning), elektronisk signatur (säker utfärdare) samt kryptering (insynsskydd av information).	
10.2.1.2-1	För öppen information skall skydd finnas mot förvanskning och förlust.	10.2.1.2-1.I1
10.2.1.2-2	Personuppgifter skall skyddas med hänsyn till gällande integritets- och sekretesskrav (jämför PUL).	10.2.1.2-2.I1
10.2.1.2-3	ITP-kraven måste följas så att stadens informationstillgångar skyddas mot obehörigt intrång.	---
10.2.1.2-4	Vid införande av nya internettjänster skall alltid informationsklassi-ficering genomföras för fastställande av krav på identifieringssätt.	10.2.1.2-4.I1 10.2.1.2-4.I2

Instruktioner för informationssäkerhet vid utveckling och tillämpning av Internettjänster

10.2.1.2-1.I1

Särskild vikt skall läggas vid att koden i WEB-tillämpningar är säkrad för manipulation. Verktyg som WEBInspect eller motsvarande kan användas.

10.2.1.2-2.I1

Datainspektionens allmänna råd "Säkerhet för personuppgifter" skall följas.

10.2.1.2-4.I1

Hänvisning till 5.2.1.1.

10.2.1.2-4.I2

Om informationsklassificeringen ger en säkerhetsprofil lika med 1 för någon av klassnings-parametrarna Åtkomstbegränsning, Riktighet och Spårbarhet skall hårt certifikat användas.

Om informationsklassificeringen ger en säkerhetsprofil lika med 2 för någon av klassningsparametrarna kan antingen mjukt certifikat användas eller engångslösenord med dosa (intern användning) alternativt engångslösenord med SMS eller annan likvärdig metod.
I övriga fall skall användarid plus lösenord användas såvida inte tjänsten skall vara allmänt tillgänglig.
För mer detaljerad information hänvisas till Handbok för val av IDentifieringssätt vid extern inloggning via Internet, (HID).

10.2.2 Elektronisk signatur

I de fall utställarens identitet måste garanteras vid informationsutbyte (ex.vis via underskrift) skall rekommenderad teknisk lösning användas.

10.2.2.1 *Anvisningar för elektronisk signering*

Pos	Text	Koppling till Instruktioner
Allmänt	Elektroniska signaturer kan användas i stället för handskrivna signaturer och därmed möjliggöra elektroniska, juridiskt bindande avtal, order, betalningar och så vidare vid bland annat e-handel mellan företag/organisationer.	
10.2.2.1-1	Elektronisk signering skall ske med säkerhetsmässigt acceptabel teknik och förväntad juridisk acceptans.	10.2.2.1-1.I1

10.2.2.1-1.I1

Kompletteras när behov av elektronisk signering aktualiseras.

10.3 Säkerhet i databaser och program

10.3.1 Styrning av säkerhet i databaser och program

Hantering av databaser och program skall ske enligt fastställd systemutvecklings-/förvaltningsmodell.

10.3.1.1 *Anvisningar för hantering av testdata och program*

Pos	Text	Koppling till Instruktioner
Allmänt	All information i samband med systemutveckling och –förvaltning skall skyddas enligt samma principer som övrig verksamhetsinformation.	
10.3.1.1-1	Kopiering av produktionsdata skall loggas för att erhålla spårbarhet.	10.3.1.1-1.I1
10.3.1.1-2	Data i testmiljö får ej innehålla verkliga persondata.	---
10.3.1.1-3	Före driftgodkännande skall acceptanstest vara avslutad.	---
10.3.1.1-4	Före ändringsgodkännande skall fastställd ändringsrutin vara avslutad.	---
10.3.1.1-5	All programvara (ny/ändring) skall godkännas innan installation i produktionsmiljö.	10.3.1.1-5.I1

Instruktioner för hantering av testdata och program

10.3.1.1-1.I1

Kopiering får endast ske efter skriftlig beställning från projektledare/systemägarrepresentant/systemförvaltare och skall sedan registreras i ärendehanteringssystem eller motsvarande.

10.3.1.1-5.I1

Innan installation i produktionsmiljö skall det finnas ett testprotokoll, undertecknat av systemägarrepresentant eller annan av honom/henne utsedd person.
IT-handboken, del Testhandboken skall följas.

11 Kontinuitets- och avbrottsplanering

Kontinuitets- och avbrottsplanering är förmågan och beredskapen att hantera störningar/avbrott i en organisations verksamhet.

11.1 Kontinuitetsplanering

11.1.1 Processen kontinuitetsplanering

Processen skall fokusera på aktuell verksamhets viktigaste mål/uppgifter.
Detta innebär planering och förberedelse av åtgärder som möjliggör att verksamheten kan upprätthållas trots att allvarliga störningar/avbrott inträffat.

11.1.1.1 *Anvisningar för processen kontinuitetsplanering*

Pos	Text	Koppling till Instruktioner
Allmänt	För att reducera konsekvenserna vid allvarliga störningar/avbrott i verksamheter med starkt IT-stöd erfordras en i förväg upprättad och dokumenterad kontinuitetsplan. [Motsvarande planering för IT-verksamheten kallas avbrottsplanering].	
11.1.1.1-1	Verksamhetsansvarig chef ansvarar för att dokumenterad kontinuitetsplan finns om klassificerade system med Tillgänglighet nivå 1 eller 2 används i verksamheten.	11.1.1.1-1.I1
11.1.1.1-2	Det skall finnas en ansvarig utsedd för att hålla kontinuitetsplanen aktuell.	---
11.1.1.1-3	I SLA ingående i drift- och förvaltningsavtal skall framgå ansvarsbilden för kontinuitetsplanen.	---

Instruktioner för processen kontinuitetsplanering

11.1.1.1-1.I1

Om en allvarlig störning/avbrott inträffar i en verksamhet kommer mycket stora och speciella krav att ställas på all berörd personal. Många svåra och snabba beslut måste fattas i en pressad arbetssituation. För att begränsa skadeverkningarna i verksamheten är det därför av avgörande betydelse att man i förväg har fastställt den organisation som skall fungera när hela eller delar av kontinuitetsplanen måste aktiveras.
En funktion som måste ges hög prioritet är information till personal, användare, kunder och massmedia.

Kontinuitetsplanen skall omfatta:
- ansvar och befogenheter för kritiska rollinnehavare
- informationskanalerna, vem man informerar

- reservplaner för olika händelser
- plan för återgång till normalläge
- plan för återtagning av förlorad information och annat av vikt
- rutin för vidmakthållande av kontinuitetsplanen

11.2 Avbrottsplanering

11.2.1 Processen avbrottsplanering

Processen skall fokusera på återstart av IT-system enligt fastställd prioritetsordning.

11.2.1.1 *Anvisningar för processen avbrottsplanering*

Pos	Text	Koppling till Instruktioner
Allmänt	För att reducera konsekvenserna vid allvarliga produktionsstopp erfordras en i förväg upprättad och dokumenterad avbrottsplan.	
11.2.1.1-1	Tekniskt systemansvarig ansvarar för att dokumenterad avbrottsplan finns om klassificerade system med Tillgänglighet nivå 1 eller 2 används i verksamheten och där maximal avbrottstid understigande 1 vecka gäller.	11.2.1.1-1.I1
11.2.1.1-2	Tekniskt systemansvarig ansvarar för att hålla avbrottsplanen aktuell.	---

Instruktioner för processen avbrottsplanering

11.2.1.1-1.I1

Avbrottsplanen skall omfatta:
- ansvar och befogenheter för kritiska rollinnehavare
- informationskanalerna, vem man informerar
- reservdriftalternativ
- rutin för återstart
- eventuellt behov av utrustning/reservdelar
- rutin för vidmakthållande av avbrottsplanen

Avbrottsplanen placeras lämpligen under egen flik (avbrottshantering) i driftdokumentationen.

11.3 Riskanalyser

11.3.1 Processen riskanalys

Processen skall fokusera på hoten mot aktuell verksamhets viktigaste mål/uppgifter.

11.3.1.1 *Anvisningar för processen riskanalys*

Pos	Text	Koppling till Instruktioner
Allmänt	En riskanalys har till syfte att på ett systematiskt sätt granska och identifiera hot och risker i en verksamhet, bedöma konsekvenserna och ge åtgärdsförslag för att minimera/reducera hoten.	
11.3.1.1-1	Riskanalys skall genomföras för klassificerade system nivå 1 eller 2.	---
11.3.1.1-2	Riskanalys skall genomföras enligt av staden rekommenderad metod.	11.3.1.1-2.I1

11.3.1.1-3	Deltagare i en riskanalys skall ha kunskap och erfarenhet från den verksamhet som skall analyseras.	---

Instruktioner för processen riskanalys

11.3.1.1-2.I1
Arbetsgången kan schematiskt beskrivas på följande sätt: -identifiera hoten mot verksamheten -bedöm konsekvenserna om hoten förverkligas -fastställ vilken verksamhetsnivå som skall upprätthållas -ange vilka åtgärder som krävs i form av reservrutiner -prioritera återstartsordningen om flera system är berörda Detta förutsätter en god beskrivning av systemens inbördes samband. Beskrivning av inom staden rekommenderade metoder återfinns i Handbok för RIskanalys, (HRI).

12 Efterlevnad

En väl fungerande informationshantering bidrar till att staden kan fullgöra sina uppgifter. Det är därför viktigt att tillämpliga lagar och förordningar samt aktuella regelverk efterlevs för att störningar ej skall uppstå.

12.1 Identifiering av tillämpliga bestämmelser

12.1.1 Lagar och förordningar

Minimikraven avseende informationssäkerhet fastställs genom lagar och förordningar.

Tryckfrihetsförordningen ställer krav på att allmän handling skall vara tillgänglig.

12.1.1.1 *Anvisningar för hantering av lagar och förordningar*

Pos	Text	Koppling till Instruktioner
Allmänt	Grundnivån för informationssäkerheten inom staden styrs bl a av gällande lagar och förordningar.	
12.1.1.1-1	Tillämpliga lagar och förordningars krav måste beaktas i stadens IT-system. Nedan ges exempel på lagar som berör de flesta verksamhetsområdena inom staden: -Tryckfrihetsförordningen (SFS 1949:105) -Sekretesslagen (SFS 1980:100) -Säkerhetsskyddslagen (SFS 1996:627) -Lag om skydd för företagshemligheter (SFS 1990:409) -Bokföringslagen (SFS 1999:1078) / Lagen om kommunal redovisning (SFS 1997:614) -Arkivlagen (SFS 1990:782) -Personuppgiftslagen (SFS 1998:204) -Upphovsrättslagen (SFS 1960:729) -Lag om ansvar för elektroniska anslagstavlor (SFS 1998:112) -Lagen om kvalificerade elektroniska signatur (SFS 2000:832) Dessutom kan för vissa verksamhetsområ-	---

	den ytterligare lagar tillkomma, exempelvis -Lag om skydd för landskapsinformation (SFS 1993:1742)	
12.1.1.1-2	Arkivering och gallring skall ske i enlighet med gallringsbeslut.	12.1.1.1-2.I1
12.1.1.1-3	IT-system som hanterar personuppgifter skall vara förtecknat och anmält till person-uppgiftsombud alternativt Datainspektionen. I Stockholms stad finns ett antal centrala system som i enlighet med beslut i kommun-fullmäktige är obligatoriska för berörda förvaltningar. För IT-säkerheten i dessa system ansvarar förvaltningarna bara i den omfattning som de har befogenheter att kontrollera och åtgärda brister.	12.1.1.1-3.I1

Instruktioner gällande lagar och förordningar

12.1.1.1-2.I1

Med stöd av Arkivnämndens allmänna anvisningar om gallring kan beslutas vilka handlingar som kan gallras. Gallringsplaner upprättas och beroende på typ av handling anges vad som skall gallras och när det skall ske.
Exempel:

Handling	Gallringsfrist	Anmärkning
Register av tillfällig betydelse	Vid inaktualitet	Till exempel kalendrar och telefonlistor som ej behövs för återsökning av ärenden eller för dokumentation av verksamheten.

12.1.1.1-3.I1

Säkerhet för personuppgifter regleras i PUL §31 samt i Datainspektionens allmänna råd, Säkerhet för personuppgifter.

12.2 Granskning av säkerhetspolicy, etik och teknisk efterlevnad

12.2.1 Kontroll av säkerhetspolicy och etik

Uppföljning av Internetanvändandet skall göras för att kontrollera om anvisningar och/eller etiska normer efterlevs.
Uppföljning i övrigt kan ske på olika sätt beroende på typ av verksamhet.

12.2.1.1 *Anvisningar för åtkomst till och användning av Internet*

Hänvisning till 6.1.1.3.

12.2.1.2 *Anvisningar för säkerhetsuppföljning*

Pos	Text	Koppling till Instruktioner
Allmänt	Metodiken för att genomföra uppföljningar kan variera men några vanliga tillvägagångssätt är bland annat: - intern uppföljning med eller utan hjälp av IT-stöd - internrevision (oftast uppföljning av åtkomst, sk Auditing) - traditionell uppföljning/revision med hjälp av externa konsulter	

	- attacksimulering/intrångsförsök av externa konsulter Initiativtagare till säkerhetsuppföljningen kan vara informationssäkerhetschef, informationssäkerhetssamordnare eller verksamhetsansvarig chef Beroende på karaktären av uppföljning varierar bemanningen vid uppföljningstillfället.	
12.2.1.2-1	Uppföljning skall ske med av staden rekommenderad metod.	12.2.1.2-1.I1

Instruktioner för säkerhetsuppföljning

12.2.1.2-1.I1
Kontinuerlig säkerhetsgranskning/revision skall genomföras med standardiserad metod såsom ISAP eller motsvarande. Metodstöd och anvisningar kan erhållas via stadens Informationssäkerhetschef.

Förändringshistorik

Datum	Författare	Granskat av	Fastställd av	Beskrivning
2005-11-30	C Daun	Kent Larsson	Stadsdirektör	Grundversion